Penerapan Kriptografi Pada Pengamanan Pengiriman Pesan Pada Sosial Media Dengan End-To-End Encryption

Haikal Ardzi Shofiyyurrohman - 13521012[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]13521012@stei.itb.ac.id

***Abstrak*—Dengan adanya internet, pertukaran pesan melalui media sosial sudah menjadi salah satu kebutuhan utama bagi masyarakat global dalam berkomunikasi namun, maraknya kebocoran data pada internet membuat masyarakat pengguna media sosial khawatir dengan keamanan privasi dari lalu lintas pertukaran pesan pada internet. Oleh karena itu, Beberapa media sosial seperti, *WhatsApp, line,* dan media sosial lainnya menggunakan *End-To-End Encryption* untuk menjaga privasi dari pertukaran pesan yang digunakan oleh masyarakat. *End-To-End Encryption* bekerja dengan menggunakan konsep enkripsi dari kriptografi yang berjenis kriptografi asimetris, yaitu *Public-Key Cryptography* untuk mengamankan pesan yang dikirim pengguna dengan cara mengubah pesan menjadi *ciphered text* dengan *Public-Key Encryption* agar saat pesan tersebut melewati jaringan internet informasi yang terkandung pada pesan tidak dapat dibaca dan pada saat pesan tersebut sampai pada tujuan maka pesan tersebut akan diubah kembali menjadi pesan asalnya dengan menggunakan *Private-Key Decryption*.**

***Keywords*—kriptografi, media sosial, pesan, keamanan.**

I. PENDAHULUAN

Pada zaman modern ini, jarak tidak lagi menjadi halangan untuk seseorang untuk berkomunikasi. Dengan banyaknya aplikasi media sosial pertukaran pesan dan dibantu dengan adanya internet, seseorang hanya perlu mengirim pesan melalui gawai atau komputer yang dimiliki dan pesan tersebut secara singkat mampu diterima oleh penerima pesan terlepas seberapa jauh jaraknya. Akan tetapi, karena internet mampu diakses oleh siapapun, maka sangat rentan berpotensi terjadinya *data breach* yang dilakukan oleh *pihak-ketiga* pada pesan tersebut yang dapat menyebabkan pengeksploitasian informasi sensitif pengguna, tersebarnya informasi palsu (*hoax*), *impersonation* (berpura-pura menjadi kerabat seseorang untuk mengeksploitasi orang tersebut), hingga penipuan. Oleh karena itu, pengamanan pesan secara menyeluruh sangat dibutuhkan pada aplikasi media sosial tersebut.

Pengamanan pesan umumnya menggunakan kriptografi. Kriptografi memiliki tiga jenis, yaitu kriptografi simetri, kriptografi asimetri, dan *hashing*. Pada media sosial pengamanan biasanya menggunakan kriptografi asimetris karena dinilai jauh lebih aman dibandingkan dengan kriptografi simetri dan mampu dibalikan kembali menjadi plainteks jika dibandingkan dengan *hashing*. Ada banyak media sosial yang menggunakan kriptografi asimetri.

II. LANDASAN TEORI

A. Kriptografi

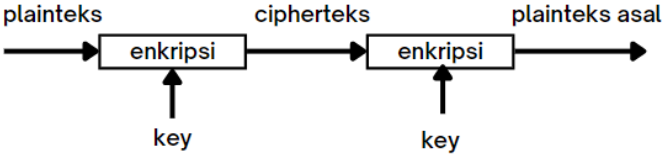
Gambar 2.1 Kriptografi Mesir kuno 3000 SM
(sumber: www.123rf.com)

Kriptografi berakar dari Bahasa Yunani yang artinya *secret writing*, adalah ilmu dan seni untuk merahasiakan suatu pesan dengan mengacak isi pesan agar tidak dapat dibaca oleh pihak yang tidak berhak [1]. Dalam sejarah, kriptografi paling tua dapat ditemukan sekitar 3000 tahun sebelum Masehi pada bangsa Mesir, mereka menggunakan hieroglif untuk menyembunyikan pesan mereka yang berupa tulisan dari orang yang tidak berhak [2]. Pada saat ini, pesan yang dikirim tidak hanya tulisan, tetapi juga gambar, audio, dan juga video sehingga pada saat ini, kriptografi sudah menjadi sangat berkembang sehingga bentuk pesan seperti, gambar, audio, dan video dapat dirahasiakan. Namun, pada kriptografi dikenal pula ilmu atau cara untuk memecah pesan tersebut yang dinamakan sebagai kriptoanalisis.

Dalam kriptografi modern, teknik yang digunakan untuk merahasiakan pesan diperoleh dari konsep matematika dan beberapa aturan yang berdasarkan perhitungan untuk mengubah pesan menjadi sulit untuk di pecah. Konsep dan aturan inilah yang digunakan sebagai algoritma pembuat kunci, verifikasi

untuk keamanan data pribadi, untuk keamanan transaksi rahasia seperti kartu kredit dan transaksi kartu debit. Berikut lima istilah penting yang ada pada kriptografi:

1. Plainteks (P) adalah pesan asli yang perlu dirahasiakan,
2. Cipherteks (C) adalah hasil dari pesan yang sudah dirahasiakan,
3. Key (K) adalah kunci yang berupa pengaturan pengacakan pesan yang hanya diketahui oleh pengirim dan penerima,
4. Enkripsi ($E_k(P)$) adalah proses penyandian plainteks menjadi cipherteks dengan kunci,
5. Dekripsi ($D_k(C)$) adalah proses pengembalian cipherteks menjadi plainteks [3].



Gambar 2.2 Proses enkripsi dekripsi (sumber: Matematika Diskrit, Rinaldi Munir).

Kriptografi memiliki empat tujuan dasar:

1. Kerahasiaan, informasi hanya dapat diakses oleh orang yang berhak dan tidak ada siapapun selain orang tersebut yang bisa mengakses.
2. Integritas, Informasi tidak dapat diubah dalam penyimpanan atau saat pengiriman antara pengirim dan penerima yang berhak tanpa tambahan pada informasi tanpa terdeteksi.
3. Anti-Penyangkalan, Pengirim pesan tidak bisa menyangkal bahwa dia bukan yang mengirim informasi pada kemudian waktu.
4. Autentikasi, Identitas dari pengirim dan penerima dapat diketahui, juga titik awal dan titik akhir dari informasi pun dapat diketahui [7].

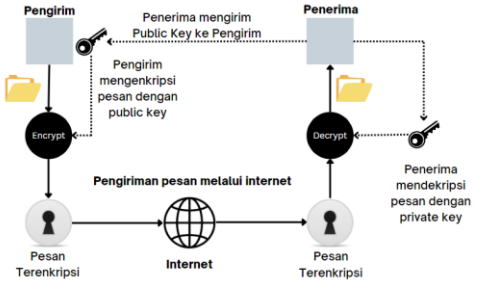
Dari cara pengenkripsiannya, kriptografi dibagi menjadi tiga, yaitu:

1. Kriptografi simetri, menggunakan satu kunci yang sama untuk mengenkripsi dan mendekripsi.
2. Kriptografi asimetri, menggunakan dua kunci yang berbeda dengan satu kunci mengenkripsi dan kunci lainnya mendekripsi.
3. *Hashing*, memetakan data ukuran berapapun ke string bit dari ukuran tetap.

B. Kriptografi Asimetri

Kriptografi Asimetri pertama kali diusulkan oleh Whitfield Diffie dan Martin Hellman pada makalah mereka yang berjudul *New Direction in Cryptography* pada tahun 1976 yang usulannya pada saat ini dikenal sebagai *Diffie-Hellman key exchange* yang dibuat untuk menyelesaikan masalah pendistribusian kunci pada kriptografi simetri [4]. Kriptografi asimetri memiliki dua kunci yang diperlukan dalam pengenkripsian:

1. Kunci publik, penerima pesan mengirimkan suatu kunci ke pengirim melalui internet untuk mengenkripsi pesan tersebut, namun kunci ini tidak bisa dipakai untuk mendekripsi pesan tersebut.
2. Kunci privat, penerima lalu mendekripsi pesan yang telah diterima dengan kunci privat.



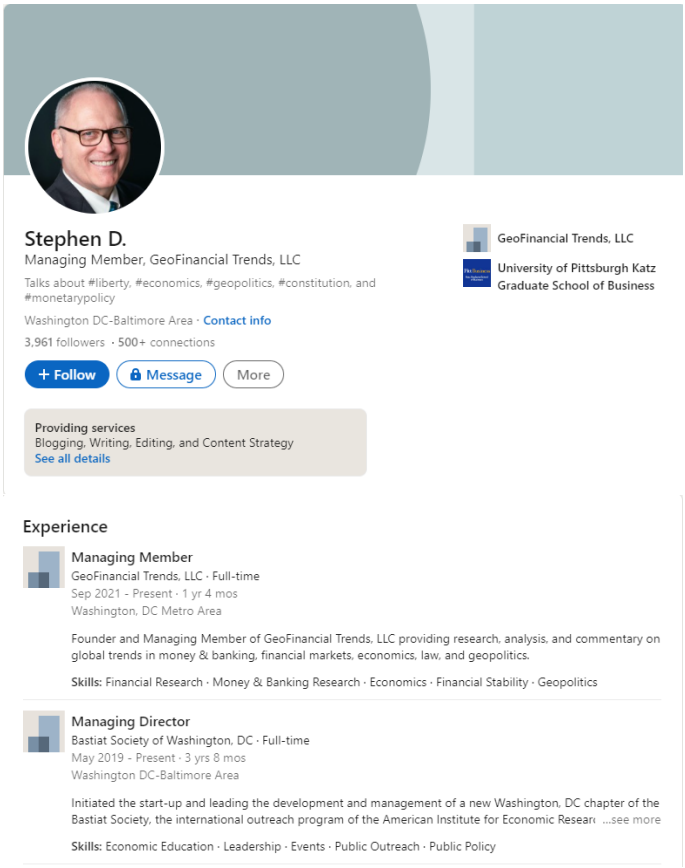
Gambar 2.3 Proses enkripsi kriptografi asimetri (sumber: Dokumen penulis).

C. Media Sosial

Gambar 2.4 Sosial Media (Sumber: https://pict.sindonews.net/dyn/732/pena/news/2022/06/13/207/797139/media-sosial-dengan-pengguna-terbanyak-di-indonesia-dan-dunia-jry.jpg)

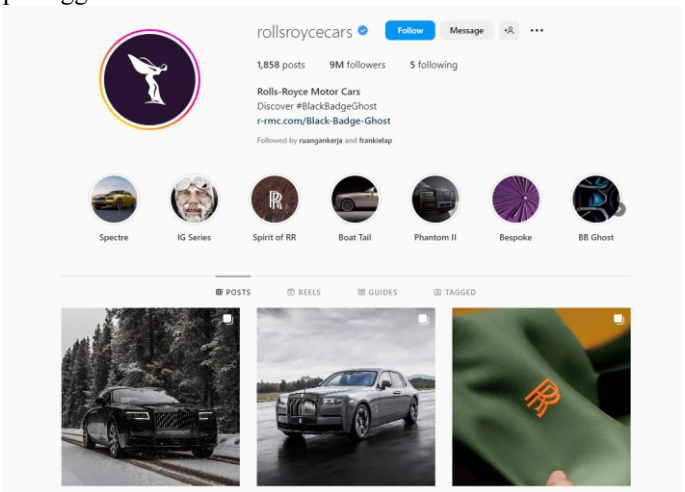
Media Sosial adalah sebuah media untuk bersosialisasi satu sama lain dan dilakukan secara daring dan memungkinkan manusia saling berinteraksi tanpa dibatasi ruang dan waktu [2]. Media sosial itu berbasis internet dan memberikan pengguna konten komunikasi secara cepat, seperti informasi pribadi, dokumen, *video*, dan foto. Pengguna mengakses media sosial lewat gawai mereka seperti, ponsel, komputer, laptop, dan lain-lain. Media sosial memiliki saat ini mengimplementasikan berbagai variasi dari teknologi penunjang aktivitas, seperti *photo sharing*, *blogging*, permainan sosial, jaringan sosial, *video sharing,* jaringan bisnis, dunia virtual, ulasan, dan masih banyak lagi. Media sosial saat ini sudah digunakan oleh berbagai kalangan di masyarakat, bahkan pemerintah dan politisi menggunakan media sosial untuk berkomunikasi dengan masyarakat.

Untuk individu, media sosial digunakan untuk saling berkomunikasi dengan keluarga, kerabat, dan teman dekat. Beberapa orang juga menggunakan media sosial untuk mencari kesempatan pekerjaan, mempromosikan karir pribadinya, mencari orang yang memiliki ketertarikan yang sama terhadap sesuatu dan membagikan pikiran, emosi, dan perasaan mereka. Mereka yang terlibat dalam aktivitas ini adalah termasuk ke dalam bagian jaringan sosial virtual.



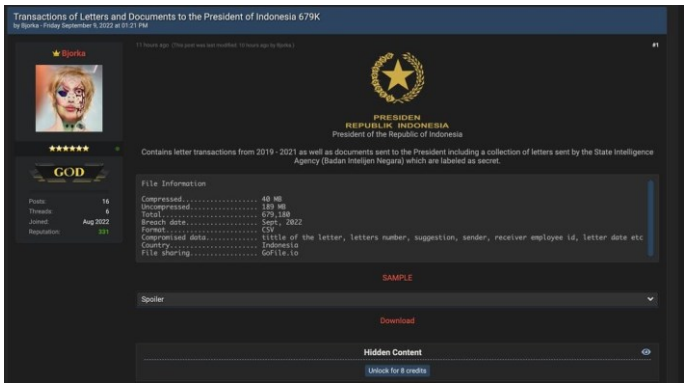
Gambar 2.6 Medsos sebagai sarana mempromosikan karir
(sumber: LinkedIn)

Untuk bisnis, media sosial merupakan alat yang sangat berguna untuk menjangkau pasar yang jauh lebih luas. Perusahaan menggunakan media sosial untuk mencari dan berkomunikasi dengan pelanggan, promosi dan pengiklanan, melihat trend yang ada pada konsumen, dan menawarkan layanan dan bantuan kepada konsumen. Sosial media sangat membantu perkembangan bisnis saat ini, karena sosial media memfasilitasi komunikasi dengan pelanggan, menghadirkan interaksi sosial yang lebih dekat antara perusahaan dengan pelanggan.



Gambar 2.7 Perusahaan mempromosikan produknya di sosial media
(Sumber: Instagram)

D. *Data breach*



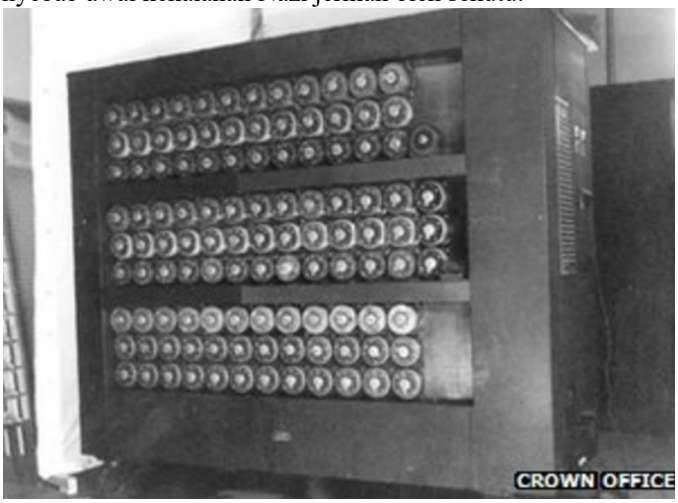
Gambar 2.5 Pembobolan data oleh peretas
(sumber: https://www.youtube.com/watch?v=lXhwEXMoS5Q)

Data Breach adalah hasil dari serangan siber yang mana penjahat mendapatkan akses illegal ke sistem gawai atau jaringan dan mencuri informasi finansial atau rahasia personal yang sensitif, rahasia, dan personal. Kebocoran data seringkali pasti berakhir di *dark web*, yang mendorong terjadinya kejahatan siber seperti, pemecahan sandi, eksploitasi informasi penting, dan penipuan.

Gambar 2.8 Mesin cipher enigma
(Sumber: https://www.bbc.com/news/technology-18419691)

Data breach pada zaman dahulu, sama seperti pembocoran informasi seperti surat kenegaraan, surat perintah militer, pencegatan sandi morse dari radio, jika informasi dalam transmisi tersebut terenkripsi, maka yang membocorkan data akan melakukan kriptoanalisis untuk memecah informasi tersebut dan mengeksploitasinya. Salah satu pembocoran paling berpengaruh dan menjadi pelopor banyak sekali kemajuan teknologi adalah pembocoran sandi *enigma* Nazi oleh Alan Turing dari Inggris. Ia menciptakan suatu mesin yang dapat

memecahkan kombinasi dari kode sandi *enigma* dengan instan dan mampu melihat isi dari sandi tersebut, yang menjadi penyebab awal kekalahan Nazi jerman oleh sekutu.



Gambar 2.9 Mesin Pemecah Enigma Alan Turing
(sumber: https://www.bbc.com/news/technology-18419691)

Pada media sosial, para penjahat siber biasanya menarget para pekerja perusahaan bisnis atau konsumen dari perusahaan tersebut dengan *impersonating* (berpura-pura) sebagai representative dari perusahaan tersebut dengan niat untuk mendapatkan informasi penting mereka.

E. End-To-End Encryption

End-To-End Encryption adalah metode pengamanan komunikasi yang mencegah *pihak-ketiga* dari pengaksesan pesan pada saat pengiriman pesan berlangsung. *End-To-End Encryption* ini secara luas banyak digunakan oleh banyak aplikasi media sosial yang mempunyai fitur *chatting*. Dalam *End-To-End Encryption,* data dienkripsi oleh pengirim dan hanya penerima yang dapat mendekripsikannya dengan kunci kriptografi rahasia [5].

End-To-End Encryption dinilai lebih aman daripada enkripsi pada umumnya karena pada saat proses pengiriman berlangsung pesan dapat diakses namun tidak dapat dibaca atau dirusak oleh apapun atau siapapun bahkan penyedia layanan itu sendiri. Dengan menggunakan strategi *End-To-End Encryption* ini membuat data pribadi pengguna aplikasi yang masif dan sulit diamankan tersebut menjadi jauh lebih aman sehingga membangun kepercayaan terhadap pengguna aplikasi media sosial tersebut [6].

End-To-End Encryption menjaga data pengguna dari dua hal yaitu, kebocoran data, dan perusakan data, namun, *End-To-End Encryption* tidak mampu menjaga data pengguna dari:

1. Metadata, setiap pesan yang terkirim tidak hanya membawa informasi dalam pesan tersebut, tetapi juga informasi tentang pesan tersebut seperti waktu dikirimnya pesan tersebut. Hal ini dapat menjadi kesempatan bagi *pihak-ketiga* untuk mencari cara mencegat pesan tersebut setelah terdekripsi,
2. Bocornya titik-awal atau titik-akhir, jika *pihak-ketiga* mampu melihat pesan tersebut sebelum terenkripsi, contohnya meretas gawai pengguna dan melihat pesan yang tidak terenkripsi [5].

Manfaat utama dari *End-To-End Encryption* adalah pencegahan data yang ditransmisi untuk dibaca selain dari penerima. Selain itu, manfaat dari *End-To-End Encryption* adalah pesan yang terenkripsi tidak dapat dibaca oleh siapapun selain penerima dan tidak ada siapapun yang bisa mendekripsikannya. Metode data enkripsi modern dirancang dengan sedemikian rupa yang jika data yang terenkripsi berubah, maka pesan menjadi tidak bermakna, secara instan memberi tahu perubahannya. Tidak ada cara apapun untuk melakukan perubahan pada data tersebut. Dengan hal tersebut, *End-To-End Encryption* menegaskan konsistensi dari komunikasi pengguna. Jika pengguna berhasil menerima pesan yang terdekripsi, maka pengguna dapat memastikan bahwa pesan yang diterima adalah pesan asli yang dikirim dari asalnya, bukan pesan yang telah diubah.

III. PEMBAHASAN

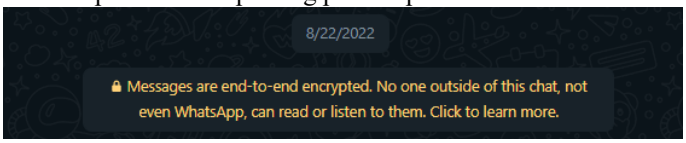
A. Cara Kerja *End-To-End Encryption*

End-To-End Encryption digunakan jika keamanan data diperlukan, termasuk finansial, kesehatan, dan industri komunikasi. Seringkali digunakan untuk membantu perusahaan dalam mengatasi masalah privasi data, dan regulasi dan hukum dari keamanan [6]. Cara terbaik untuk memahami *End-To-End Encryption* ialah dengan membandingkan dengan sistem enkripsi yang lebih tradisional yaitu, *encryption-in-transit*. Umumnya, jika suatu layanan menggunakan enkripsi, data akan dienkripsi pada gawai pengirim lalu mengirimnya ke server. Pada server, data akan didekripsi untuk proses validasi data, dan setelahnya dienkripsi kembali. Data tersebut dienkripsi kapanpun pada saat pengiriman tetapi, didekripsi saat sedang proses validasi di server. Hal ini membuat kerentanan yang membuat informasi dapat diakses oleh peretas, dan pencuri informasi.

Sebaliknya, *End-To-End Encryption* melakukannya dengan mengenkripsi data pada gawai pengirim dan tidak akan didekripsi sampai data tersebut mencapai tujuannya, bahkan layanan yang mengirim data tersebut tidak dapat melihat isi dari data yang dikirim saat melalui server. Hal ini penting, karena *End-To-End Encryption* memberikan pengguna kepercayaan bahwa komunikasi mereka aman dari *pihak-ketiga* bahkan penyedia layanan itu sendiri.

B. Contoh Penerapan Algoritma End-To-End Encryption Suatu Pesan Pada Media Sosial WhatsApp.

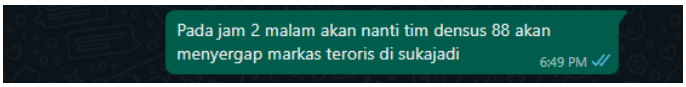
Pada media sosial *WhatsApp* seluruh pengguna dapat melihat pemberitahuan jenis enkripsi digunakan oleh media sosial tersebut pada awal tiap ruang percakapan.



Gambar 3.1 Pemberitahuan keamanan dengan enkripsi yang digunakan
(sumber: Dokumen Penulis)

Mekanisme pengenkripsian adalah sebagai berikut:

1. Pengirim akan mengirim suatu pesan *(plainteks)* dengan contoh gambar berikut:



Gambar 3.2 plainteks dari pengirim
(sumber: Dokumen Penulis)

2. Pada saat pengguna menekan tombol pengiriman, maka gawai penerima akan mengirimkan suatu kunci yang akan menjadi kunci enkripsi pesan dari pengirim, contoh kunci untuk pengenkripsian adalah dengan kunci dibawah ini dengan Public Key dengan skema *encoding* base64:

MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDMG h2EUgSLjc4NhktVgzKf5SAxON0BSW6gC4+oqHxYaGnMVO QBQ/Q2DeSLApHwtonY6gKeICN8hdgLMqqrE+YLRpITxCb9 ZVDF0krZsqqLEm9k097wVTYpSHqRBmD+uK6Kuu95mtezYa lFlb6gMeYM/xC/oieXQduyiulyC3h+7QIDAQAB

3. Lalu setelah dienkripsi maka akan dihasilkan cipherteks berikut:

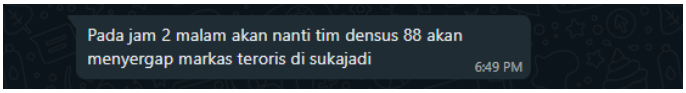
DQK3dyqZ9s0zx1Xq1lWEJKIC5QdqcY4Z+ZasR3KyovE9w+q PKBO9F1PFMQWiiz8aP7XCcJOlwSysFSR1goOAOd5g/ScT2 AK6sdfGRxP4qvru2DACRNvxM1fFx6gYMZuvbpNYHyH3S+5 87SpXCOZ7NqbQBKpqOt23zQWvzSYiP2w=

4. Cipherteks lalu akan dikirimkan ke penerima melalui server, dengan teks tersebut siapun tidak akan bisa memecahkan cipherteks tersebut karena diperlukannya pasangan kunci dari *public key* yang hanya dimiliki oleh penerima, bahkan *WhatsApp* sebagai penyedia layanan tidak dapat memecahkan cipherteks tersebut.

5. Setelah diterima oleh penerima, maka gawai penerima akan mendekripsikan cipherteks dengan *private key*, contoh *Private Key* dengan skema *encoding* base64:

MIICdgIBADANBgkqhkiG9w0BAQEFAASCAmAwggJcAg EAAoGBAMwaHYRSBIuNzg2GS1WDMp/lIDE43QFJbqALj 6iofFhoacxU5AFD9DYN5IsCkfC2idjqAp4gI3yF2AsyqqsT5gt GkhPEJv1lUMXSStmyqosSb2TT3vBVNilIepEGYP64roq673 ma17NhqUWVvqAx5gz/EL+iJ5dB27KK6XILeH7tAgMBAA ECgYEAkXDmqbz8ainRtIeHNVd5gsF2sDyyGFGomDnE1E3 D1ggJpEa190TiSIab3oclUh/xmPYgiWejgf+qlUg0oBZc7VQN GXzz7mkX/n0jolfu/jNHac1p81uq9BT/2mS3oH5cAd5+SMbS pKiIlDEJ+95ikbKLPCGUxjGFIGN+BeVWSKECQQDtFqB5 VYbKD5JVOaBU94WPLddh9UEqlLk2gmrZDiW/aPKkAAI RnM4hd7hIy+X24671uLDLb35cW4RrUShC9woFAkEA3GH nG+MiXoxfq4/uNYRIs0AT1x3ypera9S91ByTDDAyh+GbQC B+KDnkxjN/jLp+suE2clcc2I7+5bQ3j3D/tyQJAHpZHt7+f9xu RLmuT0sJoObOZUOr6MEslpfGnZT9dAVfBzgSuP6VyNoEi hkm/7l0rakocjPJiY/numIXM4u7KHQJAPfb9H1c247S+daOri 7qdImFi8rpF7qbhV803L4IDoZCvvgNSfOY5UCZ9aynMW+ CjlNKls2tm6phOz733EoebGQJAHVhlf86Mcln01pMfJ6Rk8o njgWpDMwavuPkUY5yYXs/I9Gv1auilmC1EdzyyngixHfzm/ pBXn6mIP3RkC8xD1g==

6. Dari pendekripsian tersebut maka, akan ditampilkannya pesan asli dari pengirim:



Gambar 3.3 plainteks yang diterima penerima
(sumber: dokumen pribadi)

Dari langkah-langkah diatas dapat diketahui bahwa tidak mungkin siapapun dapat memecah ataupun merusak pesan yang ditransmisikan.

IV. KESIMPULAN

Di zaman modern yang serba cepat ini, Efisiensi pertukaran informasi menjadi prioritas utama, jarak dan waktu sudah tidak lagi menjadi halangan bagi siapapun untuk mengirimkan pesan secara instan. Dengan adanya sosial media dan dibantu dengan cepatnya transmisi data internet membuat hal tersebut menjadi terwujud namun, kejahatan dalam privasi menjadi hal yang sangat mengganggu dan berbahaya bagi pengguna media sosial karena informasi sedikit apapun dari siapapun dapat dimanfaatkan untuk bisa mendapatkan keuntungan pribadi. Oleh karena itu, diperlukannya keamanan pesan yang tidak dapat dipenetrasi oleh siapapun, bahkan pembuat layanan itu sendiri, agar hak mendapatkan privasi dalam melakukan percakapan di media sosial menjadi hal yang dipercaya oleh pengguna. *End-To-End Encryption* menjadi pengaman yang mutakhir karena hak privasi dari para pengguna bisa terpenuhi dengan sistem keamanan yang tidak bisa tembus oleh siapapun bahkan penyedia layanan tersebut.

V. UCAPAN TERIMA KASIH

Puji dan syukur penulis panjatkan kepada Tuhan Yang Maha Esa atas berkat dan rahmat-Nya makalah ini dapat diselesaikan penulis dengan tepat waktu. Penulis ingin berterima kasih kepada orangtua penulis yang selalu memberikan dukungan dari segala sisi, penulis juga ingin berterima kasih kepada dosen pengampu mata kuliah IF2120 Matematika Diskrit, Bapak Dr. Ir. Rinaldi Munir, M.T. atas ilmu yang telah disampaikan dan atas bimbingannya selama satu semester ini. Tidak lupa, penulis juga berterima kasih kepada teman-teman dari IF K03 yang selalu bersedia membantu dan menemani penulis selama satu semester ini. Penulis harap makalah ini dapat memberikan manfaat bagi para pembaca.

REFERENCES

[1] R. Munir, "IF2120 Matematika Diskrit," 2020. [Online]. Available: https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2020-2021/Teori-Bilangan-2020-Bagian3.pdf. [Accessed 10 Desember 2022].

[2] R. S. Rustian, "Apa itu Sosial Media," Universitas Pasundan, 1 Maret 2012. [Online]. Available: https://www.unpas.ac.id/apa-itu-sosial-media/. [Accessed 11 Desember 2022].

[3] R. Munir, Matematika Diskrit, Bandung: INFORMATIKA Bandung, 2010.

[4] J. Lake, "What is the Diffie–Hellman key exchange and how does it work?," comparitech, 23 Maret 2021. [Online]. Available: https://www.comparitech.com/blog/information-security/diffie-hellman-key-exchange/. [Accessed 11 Desember 2022].

[5] B. Lutkevich, "end-to-end encryption," TechTarget, Juni 2021. [Online]. Available: https://www.techtarget.com/searchsecurity/definition/end-to-end-encryption-E2EE. [Accessed 11 Desember 2022].

[6] Fornetix, "End-to-End Social Media Encryption Strategies," Fornetix, 7 Agustus 2022. [Online]. Available: https://www.fornetix.com/articles/end-to-end-encryption-strategies-becoming-the-norm-for-social-media/. [Accessed 11 Desember 2022].

[7] M. Riadi, "Pengertian, Sejarah, dan Jenis Kriptografi," KAJIANPUSTAKA.COM, 13 Januari 2014. [Online]. Available: https://www.kajianpustaka.com/2014/01/pengertian-sejarah-dan-jenis-kriptografi.html. [Accessed 12 Desember 2022].

[8] L. Johnson, Security Control Evaluation, Testing, and Assessment Handbook (Second Edition), Academic Press, 2020.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 12 Desember 2022

Haikal Ardzi Shofiyyurrohman, 13521012